Lindsey Lodge Hospice

Information Security Policy

Contents

1 Introduction

1.1 Background

Information processing forms a fundamental part of the services that are provided by Lindsey Lodge Hospice. Therefore, it is important that the organisation has a clear and relevant Information Security Policy to allow it to comply with relevant information legislation.

The purpose of Lindsey Lodge`s Information Security policy is to protect all information assets to a consistently high standard. The policy covers security which can be applied through technology but perhaps more crucially; it encompasses the behaviour of the people who manage information in the line of business.

Information security is primarily about people but is facilitated by the appropriate use of technology. The business benefits of this policy and associated guidance are:

- Assurance that information is being managed securely and in a consistent and corporate manner.
- Assurance that the organisation is providing a secure and trusted environment for the management of information used in delivering its business.
- Clarity over the personal responsibilities around information security expected of staff when working on Lindsey Lodge Hospice business.
- A strengthened position in the event of any legal action that may be taken against Lindsey Lodge Hospice (assuming the proper application of the policy and compliance with it).
- Demonstration of best practice in information security.
- Assurance that information is accessible only to those authorised to have access.
- Assurance that risks are identified and appropriate controls are implemented and documented.

1.2 Aim

Lindsey Lodge Hospice's information security policy aims to ensure that its information systems are properly assessed for security and that the following aspects of the systems are preserved:

- **Confidentiality** - Access to Data shall be confined to those with appropriate authority and legitimate rights and relationships.
- **Integrity** – Information shall be complete, accurate and up-to-date. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** - Information shall be available and delivered to the right person, at the time and place when it is needed.

1.3 Objectives

The objectives of this policy is to establish and maintain the security and confidentiality of information, patient information, donor information, information systems, applications and networks held by Lindsey Lodge Hospice by:

- Ensuring that all members of staff are aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other Information Governance policies.

- Describing the principles of security and explaining how they shall be implemented in the organisation. Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.

- Creating and maintaining within the organisation, a level of awareness of the need for Information Security as an integral part of the day to day business.

- Protecting information assets under the control of the organisation.

1.4 ISO27001

Our IT is provided by Care Plus IT Group and they have adopted the ISO27001:2005 standard for Information Security. It formally specifies an Information Security Management System (ISMS) that allows Information Security to be explicitly managed, monitored and controlled, minimising risk and ensuring compliance.

This Security Policy has been written to be compliant with ISO27001.

2 Scope

This policy applies to all staff, information, information systems, networks, applications and locations within Lindsey Lodge Hospice or supplied under contract to it.

The policy relates to information held in both manual and electronic form.

3 Roles and Responsibilities

3.1 Chief Executive

Information Security applies to all staff, although responsibility ultimately resides with the Chief Executive. This responsibility is discharged through the designated roles of Senior Information Risk Owner (SIRO) and Caldicott Guardian (Medical Director) as required by the Information Governance Toolkit.

3.2 Senior Information Risk Officer (SIRO)

The Senior Information Risk Owner (SIRO) is responsible for information risk within Lindsey Lodge Hospice and advises the Quality Assurance Group on the effectiveness of information risk management across the Organisation. This role is held by our Finance Manager.

3.3 Caldicott Guardian

The Caldicott Guardian will:

- Have lead responsibility for information security management within Lindsey Lodge Hospice acting as a central point of contact on information security for staff and external organisations.
- Manage and implement this policy and related procedures.
- Monitor potential and actual security breaches.

This role is held by our Medical Director.

3.4 IT Support Officer

The IT Support Officer will:

- Ensure that staff are aware of their responsibilities and accountability for information security.
- Ensure compliance with relevant legislation and regulations.
- Ensuring staff have appropriate training for the systems they are using.
- Ensuring staff know how to access advice on information security matters.
- Determining the level of access to be granted to specific individuals.

3.5 Line Managers/Team Leaders

Line Managers/Team Leaders shall be individually responsible for the security of their physical environments where information is processed or stored. Furthermore, they are responsible for:

- Ensuring that all staff, permanent, bank, volunteers, are aware of the information security policies, procedures and user obligations applicable to their area of work.
- Ensuring that all staff, permanent, temporary and contractors, are aware of their personal responsibilities for information security.
- Ensuring staff have appropriate training for the systems they are using.
- Ensuring staff know how to access advice on information security matters.

.

3.6 All Staff

All staff are responsible for information security and therefore must understand and comply with this policy and associated guidance. Failure to do so may result in disciplinary action. In particular all staff should understand:

- What information they are using, how it should be protectively handled, stored and transferred.
- What procedures, standards and protocols exist for the sharing of information with others.
- How to report a suspected breach of information security within the organisation.
- Their responsibility for raising any information security concerns with the Caldicott Guardian

Contracts with external contractors that allow access to the organisation's information systems must be in operation before access is allowed. These contracts must ensure that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

4 Policy Framework

4.1 Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an appropriate confidentiality clause.

Information security expectations of staff shall be included within appropriate job definitions.

4.2 Security Control of Assets

All key Information Systems shall have a named Information Asset Owner (IAO) who shall be responsible for the information security of that asset.

4.3 Access Controls

Access to information shall be restricted to users who have an authorised business need to access the information and as approved by the relevant IAO/Caldicot Guardian.

4.4 Computer Access Controls

Access to IT facilities shall be restricted to authorised users who have business need to use the facilities.

4.5 Application Access Controls

Access to data, system utilities and programs source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

4.6 Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be; identified, registered and physically protected from threats and environmental hazards.

4.7 Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures with Care Plus IT Group. This will also require agreed systems and processes with third party vendors working for and on behalf of Lindsey Lodge Hospice.

4.8 Information Security Events and Weaknesses

All Lindsey Lodge Hospice information security events and suspected weaknesses are to be reported to the Caldicott Guardian immediately. Incidents should also be reported on the Incidents reporting system straight away, which stored on the L drive.

4.9 Classification of Sensitive Information

Lindsey Lodge Hospice shall implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance contained within the IG Toolkit to secure their information assets.

4.10 Protection from Malicious Software

The organisation shall use software countermeasures and management procedures to protect itself against the threat of malicious software provided by Care Plus IT Group. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation's property without permission from Care Plus IT group. Users breaching this requirement may be subject to disciplinary action.

4.11 Monitoring System Access and Use

An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis by Care Plus IT Group on behalf of Lindsey Lodge Hospice. CPG IT will put in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts.
- Investigating or detecting unauthorised use of the system.
- Preventing or detecting crime.
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training).
- In the interests of national security.
- Ascertaining compliance with regulatory or self-regulatory practices or procedures.
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act.

4.12 Business Continuity and Disaster Recovery Plans

A Business continuity plan is available (L Drive/Policies and Guidelines) and will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident.

The SIRO has a responsibility to ensure that appropriate disaster recovery plans are in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis.

4.13 Training and Awareness

Information Governance training is mandatory and all staff are required to complete annual Information Governance training.

4.14 Clear Desk and Clear Screen

Staff must ensure that the confidentiality of sensitive information is not breached whilst in their possession. Where possible, desks and other working areas shall be cleared of all restricted information when employees leave them unattended.

This also applies to confidential information stored electronically. Workstations must be locked or logged out of when left unattended, to prevent unauthorised access to the information.

5 Information Transfer

5.1 Patient Identifiable Information

Lindsey Lodge Hospice is fully committed to the Caldicott Principles regarding the protection and use of patient identifiable or service user identifiable information, namely:

- Use and transfer of such information will only take place where the purpose is fully justified
- Use and transfer will only occur when absolutely necessary
- Use the minimum required – where possible, all data should be anonymised
- Access strictly "need to know"
- Everyone must understand their responsibilities
- Understand and comply with the law
- Understand situations where the duty to share information can be as important as the duty to protect patient confidentiality

5.2 Partner Organisations

Lindsey Lodge Hospice works with partner organisations which all have a legitimate role to play in delivering care to Lindsey Lodge service users. Partners, in this context, are taken to be:

- NLAG NHS Trust
- Macmillan Nurses – Community & Hospital
- Macmillan survivorship Team (OT & Physio)
- District Nurses

- North Lincolnshire Clinical Commissioning Group (CCG)
- Local Ambulance Services
- Non Clinical and Clinical staff working in General Practice
- Other appropriate non-NHS contractors (e.g. Independent Care and Nursing Homes)

A formal Information Protection and Sharing Protocol has been developed and published which makes the standards of information protection control explicit. This document is entitled the Community Charter.

5.3 External Organisations

In addition to partner organisations, Lindsey Lodge Hospice may receive requests for person-identifiable information. Organisations requesting such information include:

- Private Healthcare providers
- Police
- Insurance companies
- Solicitors

Whilst such requests may be legitimate, Lindsey Lodge Hospice will ensure the use of such information is not abused, by applying the following principles when considering the release of the information to non-partner organisations:

- Information will not be released without the written consent of the individual concerned
- Individuals will be fully informed
  - That information is being released
  - Of the purpose(s) for which it is being used
- Individuals will be given the right to review the information being released and given the opportunity to correct or otherwise amend such information before release.

These requirements may be waived in certain conditions (e.g. as a result of a court order or police investigation) but it is important the Chief Executive or Caldicott Guardian is informed.

5.4 Removable Media

Staff should only use encrypted removable media. Users breaching this requirement may be subject to disciplinary action.

5.5 Emails

Steps should be taken to protect any person-identifiable information sent via email. Staff must abide by **Email Use Policy.- have we got one?**

5.6 Telephone

It is essential that all staff are aware of the need to check on the credentials and identity of all callers requesting patient or service user identifiable or other sensitive information.

5.7 Verbal

Staff are reminded of their obligation, under the Caldicott guidelines, to respect the privacy of individual patients or service users. This means holding conversations about patients or service users discreetly and with due regards to the sensitivity of the subject under discussion. Staff should be aware of the dangers of conversations being overheard both in the workplace and particularly when away from it. Users of mobile phones should take particular care when in public areas especially whilst on public transport.

5.8 Postal

All staff should ensure that arrangements for sending and receiving information through the post are adequate, particularly in relation to patient or service user identifiable information. The use of recorded mail or the internal NHSmail system must be considered.

5.9 Equipment Disposal

All computer hardware disposal must be via the Care Plus Group IT Department. They will ensure that data storage devices are purged of sensitive data before secure disposal. Unusable computer media (e.g. floppy disks, magnetic tapes, CD-ROMS), should be passed to the Care Plus Group IT Department for destruction.

All disposals will be in accordance with **Standard Operating Procedure 09 - Disposal of Hardware** held within the IT Department's ISO27001 Management System.

6 Associated Policies and documents

Confidentiality and Data Protection Policy
Information Governance Policy
Records Management Policy
Data Security Breach Management Policy
Email Use Policy

7 Consultation

IT & IG committee

8 Dissemination

Via Lindsey Lodge `L` drive policies/guidelines of this form.

9 Equality Act

9.1 In accordance with the Equality Act (2010), the Hospice will make reasonable adjustments in the workplace so that an employee with a disability, as covered under the Act, should not be at any substantial disadvantage. The Hospice will endeavour to develop an environment within which individuals feel able to disclose

any disability or concern which may have a long term ad substantial effect on their ability to carry out their normal day to day activities.

9.2 The Hospice will wherever practical make adjustments as deemed reasonable in light of an employee's specific circumstances and the Hospice's available resources paying particular attention to the Disability Discrimination requirements and the Equality Act (2010)

REFERENCES: Care Plus IT Group (LLH IT provider)				
Lead Author of Policy: Kay Fowler, It Support Officer **Responsible Sub-group** IT & IG committee **RATIFICATION DATE BY TRUSTEES 19th October 2017** Review interval 3 year				
TO BE REVIEWED	REVIEW COMPLETED	BY	APPROVED BY	CIRCULATION
October 2017				